DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2016-0052]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ U.S. Immigration and Customs Enforcement-015 LeadTrac System of Records

AGENCY: Department of Homeland Security (DHS), Privacy Office.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the "Department of Homeland Security/U.S. Immigration and Customs Enforcement-015 LeadTrac System of Records" and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2016-0052, by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.

- Mail: Jonathan Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Amber Smith, Privacy Officer, (202-732-3300), U.S. Immigration and Customs Enforcement, 500 12th Street, SW, Mail Stop 5004, Washington, D.C. 20536, e-mail: ICEPrivacy@dhs.gov, or Jonathan R. Cantor (202-343-1717), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background:

The Department of Homeland Security (DHS) is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the "DHS/U.S. Immigration and Customs Enforcement (ICE)-015 LeadTrac System of Records" and this proposed rule. In this rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

The LeadTrac System of Records describes the operation of an ICE information technology system of the same name, which is owned by ICE's Homeland Security Investigations (HSI) directorate. This system contains a repository of data that is ingested

on a routine or ad hoc basis from other existing sources, and an index created from that data. LeadTrac incorporates tools that allow the data to be queried, analyzed, and presented in a variety of formats that can help illuminate relationships among the various data elements. The purpose of LeadTrac is to help ICE HSI personnel conduct research and analysis using advanced analytic tools in support of their law enforcement mission. LeadTrac Overview.

This record system allows DHS to collect and maintain information about foreign students, exchange visitors, and other non-immigrant visitors to the United Sates who overstay their period of admission or otherwise violate the terms of their visa, immigrant, or non-immigrant status (collectively, status violators), and associated organizations and individuals. Using LeadTrac, the Counterterrorism and Criminal Exploitation Unit (CTCEU) collects personally identifiable information (PII) from key Department of Homeland Security (DHS) databases and analyzes it to identify individuals who are suspected status violators. The Counterterrorism and Criminal Exploitation Unit will also use LeadTrac to collect information about organizations such as schools, universities, and exchange visitor programs being investigated by CTCEU, as well as information about individuals, including designated school officials (DSOs) and associates of suspected status violators.

ICE collects information in LeadTrac about suspected status violators and organizations to help enforce compliance with U.S. immigration laws. Specifically, the information is collected and used to support the following DHS activities: investigating and determining immigration status and criminal history information of individuals; carrying out the appropriate enforcement activity required; identifying fraudulent schools

and/or organizations and the people affiliated with the school or organization; providing HSI and ICE Enforcement and Removal Operations (ERO) with viable lead information to further investigate suspected status violators; and carrying out the required enforcement activity.

The CTCEU and Overstay Analysis Unit (OAU) personnel query a variety of DHS and non-DHS information systems and enter the results into LeadTrac to build a unified picture of an individual's entry/exit, visa, criminal and immigration history, and will comparably process information about associated individuals and organizations. Using this assembled information, CTCEU will determine which individuals or organizations warrant additional investigation for possible status violations or the operation of fraudulent institutions, and will request that the appropriate HSI field offices initiate investigations. Some of the individuals about whom ICE collects information in LeadTrac, such as DSOs and associates of suspected status violators, may have lawful permanent resident (LPR) status or be U.S. citizens.

Consistent with the Department's information sharing mission, information stored in the DHS/ICE–015 LeadTrac System of Records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/ICE information may be shared with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in the system of records notice and as otherwise authorized under the Privacy Act.

This newly established system will be included in DHS's inventory of record

systems.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

The Privacy Act allows Government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, it must issue a rule to make clear to the public the reasons why a particular exemption is claimed, and provide an opportunity to comment.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/ICE-015 LeadTrac System of Records. Some information in this system of records relates to official DHS national security, law enforcement, and immigration activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of activity techniques; to protect the identities and physical safety of

confidential informants and law enforcement personnel; to ensure DHS's ability to obtain information from third parties and other sources; and to protect the privacy of third parties. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case-by-case basis.

A system of records notice for DHS/ICE-015 LeadTrac System of Records is also published in this issue of the Federal Register.

List of Subjects in 6 CFR Part 5:

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend chapter I of title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for part 5 continues to read as follows:

Authority: Pub. L. 107-296, 116 Stat. 2135; (6 U.S.C. 101 et seq.); 5 U.S.C. 301. Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

2. Add paragraph 74 to Appendix C to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

74. The DHS/ICE-015 LeadTrac System of Records consists of electronic and paper records and will be used by ICE investigative and homeland security personnel. The DHS/ICE-015 LeadTrac System of Records contains aggregated data from ICE and

DHS law enforcement and homeland security IT systems, as well as data uploaded by ICE personnel for analysis from various public, private, and commercial sources during the course of an investigation or analytical project. This information may include some or all of the following types of personally identifiable information: identifying and biographic data such as name and date of birth; citizenship and immigration data; border crossing data; customs import-export history; criminal history; contact information; criminal associates; family relationships; photographs and other media; and employment and education information. The records also include tips received by ICE from the public concerning suspicious or potentially illegal activity, as well as telephone call detail records, which contain call transactions and subscriber data, obtained via lawful process during the course of an investigation. This information is maintained by ICE for analytical and investigative purposes and is made accessible to ICE personnel via the LeadTrac system interface. The system is used to conduct research supporting the production of law enforcement activities; provide lead information for investigative inquiry and follow-up; assist in the conduct of ICE criminal and administrative investigations; assist in the disruption of terrorist or other criminal activity; and discover previously unknown connections among existing ICE investigations.

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When a

record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2) or (k)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. Disclosure of corrections or notations of dispute may impede investigations by requiring DHS to inform each witness or individual contacted during the investigation of each correction or notation pertaining to information provided them during the investigation.

(b) From subsection (d) (Access to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another

agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose classified and other security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: August 3, 2016

Jonathan R. Cantor,
Acting Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2016-18812 Filed: 8/8/2016 8:45 am; Publication Date: 8/9/2016]